了解 ISO 26262 ASIL

QNX 软件系统公司 Chris Hobbs, Patrick Lee

汽车安全完整性等级（ASIL）不同于安全完整性等级（SIL）

ISO 26262 是从电气、电子及可编程电子安全相关系统的功能安全基本标准 IEC 61508 派生出来的。IEC 61508 定义了安全完整性等级 (SIL)，而 ISO 26262 则定义了汽车安全完整性等级 (ASIL)。或许看起来 ASIL 同 SIL 相似，而那些熟稔于构建满足 IEC 61508 SIL 认证要求安全系统的专业人士，也应能将那些方法转用于 ISO 26262 的项目上。

构建 IEC 61508 安全案例的经验以及为此收集的证据，对建立 ISO 26262 系统安全案例而言无疑是弥足珍贵的。但是，ISO 26262 不同于 IEC 61508，它“不是一个可靠性标准”，它并没有为可接受失效概率设定准确的数字。ASIL 和 IEC 61508 SIL 的定义方式是不同的。

在定义 SIL 时，IEC 61508 会考虑针对在低负荷、高负荷或连续模式下运行系统的目标失效措施。例如，一个达到连续模式 SIL 3 标准的软件组件必须拥有每小时运行低于千万分之一的风险失效概率。因此，IEC 61508 SIL 被认为是一维的，也就意味着它们只涉及规定操作模式下的失效概率。

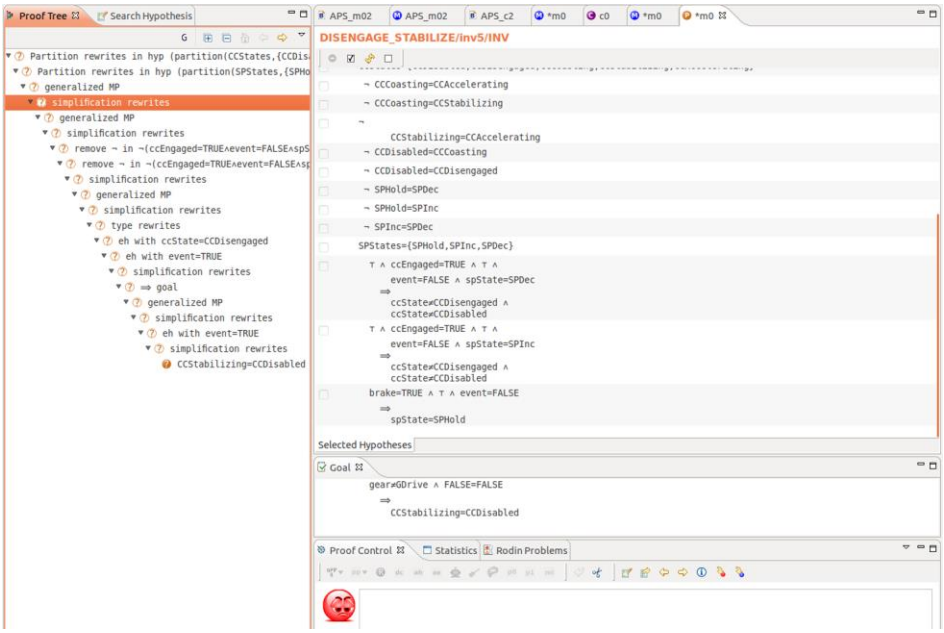
而 ASIL 则是三维的，涉及包括严重性、暴露率以及可控性在内的三个变量。ISO 26262-3 第七章“危害分析和风险评估”提供了相关的表格，将这三个变量再作细分。暴露率共有五级：“不可思议低概率”至“高概率”(E0-E4)。严重性有四级：“无伤害”至“威胁生命的伤害 (生存不确定)、致命伤害”(S0-S3)。可控性是指驾驶者的可控性，而非车辆电子系统的可控性，共有四级：“大体可控”至“控制困难或无法控制”。

该标准此章节第四个表格表明这几个变量必须结合起来，以决定车辆中电子系统、子系统或组件所要求的 ASIL。例如，某一情况具备中级发生概率 (E3)，且被视为正常可控 (C2)，但可能导致威胁生命的伤害 (S3)，那么该情况下须使用的组件应当视为 ASIL B 级。

这一定义 ASIL 的方法与 IEC 61508 所规定的严苛可靠性 (失效非概率性) 目标大相径庭。尽管 ISO 26262 在第三部分的附录 B 中给出了细节和例子，但定义 ASIL 还是要涉及众多因素，即便有了附录 B 中相关信息，也需要我们做出多种假设。

举例来说，该附件所包含的严重性等级就采用了美国汽车医学学会制定的简明创伤分级标准 (AIS)，但标准称“诸如最大简明创伤分级标准 (MAIS) 和创伤严重度评分 (ISS) 也可被采用”。类似的是，附录 B 将 C2 可控性定义为“90% 或更多的驾驶者以及其他交通参与者通常能够避免伤害”，将 E3 暴露率定义为 “平均运行时间的 1% 至 10%”

这些定义信息量大且不规范，对于建立每一组件系统的人，以及最终对于汽车制造商和供应商而言，都留有很大的自由发挥间。例如，定义 C2 可控性并没有说明 90% 是哪类驾驶者，而且它还包含了“通常”一词。



我们必须决定采用怎样的统计样本来确定 90% 的驾驶者能否在通常情况下避免伤害，也必须决定“通常”一词是否意味着超过 50%或超过 90%的发生率，或者还有其他问题需要一并考虑。暴露率同样也有赖于上下文和解读。暴露于桥上透明薄冰的概率在美国佛罗里达州和加拿大马尼托巴省是迥然不同的。

另外，该标准称对于可控性和暴露级别而言，“从一级到下一级的概率差别呈现数量级顺序”。它没有明确地说明该数量级顺序是二进制 (x2) 还是十进制 (x10)。但是从附录 B 中的案例，我们可以推断这是十进制的。例如，E1 “小于平均运行时间的 1%”，而 E2 的范围是“平均运行时间的 1% 至 10%”。

ISO 26262：一项基于目标的标准

考虑到定义一个 ASIL 我们不得不做出相应假设的数量庞大，汽车安全工程师协会 (SAE) 正草拟 J2980 — 关于 ISO26262 ASIL 危险分级的若干意见，目的是为 ASIL 三维分级提供更加明确的指导。这些指南可在我们对严重度、暴露率和可控性做各种假设时帮助减少可能性，但它们并不会消除我们定义 ASIL 时对假设的需求。

但是，如果我们退后一步，完整地去看 ISO 26262，就会注意到该标准是有关防止伤害的：

安全性目标是最高级的安全要求... 它们促成了用以避免每个危险事件不合理风险的功能安全要求。安全性目标并不是通过技术解决方案来表述的，而是以功能目标的方式呈现。

伤害可能来自众多因素，而事实上，如此繁多的因素并不能被一一列出和描述，甚至还会有遗漏。因此，构建一个不会带来不可接受伤害的 ISO 26262 系统取决于广泛的技术。ASIL 只是战略的一部分，用以帮助我们基于失效相关后果的风险性和严重度来决定某一组件所需的可靠性。

IEC 61508 是一项规范性标准，适用于高价值、小批量实施的系统，包括核电站和石油钻井平台。相反，ISO 26262 则是一项基于目标的标准，适用于价值相对较低但大批量实施的系统。ISO 26262 同其他基于目标的标准一样，这类标准针对特定环境而发展起来 (包括医疗设备、列车、汽车等)，而规范性的标准则是适用于某类系统 (例如，IEC 61508 适用于电子类)。另外，ISO 26262 表达安全要求的方式也与其他基于目标的标准相似。

举个例子，用于医疗设备的 IEC 62304 标准采用了类似于 ISO 26262 的方式，将医疗设备分为三个等级 — A 级 (没有任何伤害或健康损害)、B 级 (可能产生轻微的伤害)，和 C 级 (可能产生严重的伤害或致死) — 并将重心放在了设计、开发验证流程，以及建立安全案例的工具和技术上。这两个标准也都探讨了未针对安全相关性系统开发的系统或子系统，因为它们也会被应用到这些领域。

ASIL 要比 IEC 62304 医疗设备等级更加复杂。但相同的是，ASIL 并没有设定可靠性要求。ASIL 提供相应的指导，从而帮助我们基于伤害的概率和可接受性来建立可靠性要求。在不少案例中，我们需要根据 ISO 26262 中的信息和诸如 ALARP (最低合理可行)、GAMAB (至少总体良好)、MEM (最低限度内源性死亡率) 等各种方法，来自己设置可靠性数值。

在这种情况下，针对“无人驾驶汽车的 ASIL 将是如何”这一问题的最有效回答可能就是建立更加完善的标准，涵盖包括非人驾驶可控性在内的所有可能。如现在标准所示，无人驾驶意味着可控性将一直接近“0”，因为 ISO 26262 会将其定

义为“通过参与人的及时反应，可能借助外部措施的支持，来避免特定伤害或损害的能力”。

因此，我们将不得不把每个安全相关性组件分级为 ASIL D。就目前而言，这一答案同样适用于有人驾驶的传统汽车，若我们提出类似的问题，例如“辅助巡航控制的 ASIL 是什么？”。如果不了解 ASIL 三个维度，我们也就无从知道答案。

因此，我们必须一开始就根据 ASIL 三个维度来决定我们系统的可靠性要求：若系统失效，暴露于伤害的概率；若情况不可控，对暴露条件的可控性以及导致伤害的严重度。.

一旦我们了解了这些维度，确定 ASIL 就是一件查找第三部分表四内容的简单工作。然后，我们就可以建立自己的 ISO 26262 安全案例，展示我们的组件达到了可靠性要求，其中采用所有可利用的相关方法和证据：流程和质量管理、正式设计、代码分析、测试、针对组件的使用验证数据等。

最后，在建立安全案例时，我们不仅仅须要展示我们的系统满足了自己设定的可靠性要求，而且还要说明该可靠性是被所选 ASIL 接受的，且我们所选择的 ASIL 与已经搭建的系统相匹配。

关于 QNX 软件系统公司

QNX 软件系统公司, 黑莓公司旗下子公司，是全球领先的嵌入式互连行业操作系统、开发工具以及专业服务供应商。包括奥迪、思科、通用电气、洛克希德·马丁和西门子在内的全球技术领导者都依靠 QNX 的技术生产车用信息娱乐系统、网络路由器、医疗器械、工业自动化系统、安全与国防系统，并满足其他任务或生命关键型应用的需要。 公司成立于 1980 年，总部位于加拿大渥太华，其产品销售覆盖全球 100 多个国家。

china.qnx.com